CAB Forum London, June 2018

Browser News

1 BR Self-Assessments

We have received BR Self-Assessments from all but one CA. Thank you to everyone who completed them. We do believe that this work benefits CAs and we're considering requiring CAs to provide annual updates along with their audit documentation. An alternative being considered is to create something similar to Microsoft's Audit Letter Validation tool [1] to extract the self-assessment information from CP/CPSs. Even though, as of May 31, the BRs require all CP/CPSs to follow RFC 3647 format, We're seeing a great deal of divergence from the structure of the BRs for disclosures such as domain validation methods that would need to be cleaned up before we could automate BR Self-Assessments.

2 Email Intermediate Disclosures

Mozilla's deadline for revoking or disclosing unconstrained email intermediate certificates was April 15th. Compliance was good but not exceptional and there are a number of compliance bugs open awaiting resolution. Please ensure that none of your certificates are in the first two sections of this list: https://crt.sh/mozilla-disclosures

3 CCADB News

Current Root Store Members of CCADB: Mozilla, Microsoft, Google, Cisco, Apple

- Audit Cases now have a progress bar showing what needs to be done. The CA is responsible for completing all steps until the Audit Case reaches "Verification by Root Store". That is when Kathleen and Karina will review the Audit Case.
    - This means that CAs will now have to click on the "Audit Letter Validation [ALV]" button and resolve all errors before a root store operator will process the Case.
    - Temporary Caveat: The "Cleaned" error may be ignored for the next couple of weeks. Microsoft's team is updating this particular test.
    - The most common things that CAs usually have to fix are:
        - URLs for new audit statements must be different from the previous audit statements, and must point to a PDF file.
        - All audit statements must list the Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope.
        - The 3 test websites (valid, expired, revoked) must produce the expected result, and the SSL cert must chain up to the corresponding root cert.
- We intend to begin using ALV on intermediate certificates as well.
    - Please update the audit statements in your intermediate certificate records directly in the CCADB. If the intermediate certificate is included in the audit statement of its Issuer, then select the "Audits Same as Parent" button.

Otherwise you must update the intermediate certificate record each year with the current audit statement links.

- Audit statements for root and intermediate cert records are archived within CCADB. There is a section in the root and intermediate cert records listing the audit archives associated with it.
    - On our future/to-do list: add ability to add audit archives for older audit statements, so we could generate the full history of audit statements for a root cert. This will likely be a simplified Audit Case type of object, so CAs could upload their old audit statements, and then a root store operator could verify before CCADB processes the data.
- CCADB is being updated to account for both non-EV and EV Code Signing audits, per request from Microsoft.
- We are working to replace the old PEM->JSON tool that is used whenever someone enters PEM data into the CCADB. The new tool will be on the TLS Observatory.
    - curl https://tls-observatory.services.mozilla.com/api/v1/certificate -F certificate=@/tmp/certificate.pem
    - Kathleen recently posted about this in mozilla.dev.security.policy forum, and described the changes. Time will be given for evaluation before switching to the new tool in production and re-running on all root and intermediate cert records.
- Also on our future/to-do list: Create a Root Inclusion Case enabling CAs to directly input their data into the CCADB to request inclusion of a new root certificate, specifying which root program they are applying to. So the CA can enter their data in one place (similar to Audit Cases), and the root store operators can independently make decisions on that data.

4 Policy 2.6 Update

The latest updates to Mozilla's root store policy are being finalized with a planned effective date of 15-June. The full update is at [3] and a diff is at [4]. Major changes include:

- Section 2.2 Validation Practices now requires CAs with the email trust bit to clearly disclose their email address validation methods in their CP/CPS.
- The use of 3.2.2.5(4), the IP Address version of "any other method", has been banned for validating a domain name under 3.2.2.4(8). "Any other method" is still permitted when validating an IP Address for inclusion in a SAN.
- Methods used for IP Address validation must now be clearly specified in the CA's CP/CPS.
- Section 3.1 Audits increases the EV minimum version to 1.6.0 and removes ETSI TS 102 042 and 101 456 from the list of acceptable audit schemes.
- Section 3.1.3 Audit Parameters formalizes the requirement for an English language version of the audit statement supplied by the Auditor.
- Section 5.2 Forbidden and Required Practices moves the existing ban on CA key pair generation for TLS certificates into policy.
- Section 5.3 Intermediate Certificates requires all new intermediates created after 1-January 2019 to contain an EKU extension and to separate serverAuth from emailProtection. This means that CAs will need to create separate intermediate certificates for signing S/MIME and TLS certificates.

- Section 5.3.2 clarifies that Mozilla expects newly issued intermediate certificates to be included on the CA's next periodic audit report. As long as the CA has current audits, no special audit is required when issuing a new intermediate. This matches the requirements in BR section 8.1.
- Section 7.1 adds the following statement: "Before being included, CAs MUST provide evidence that their CA certificates have continually, from the time of creation, complied with the then-current Mozilla Root Store Policy and Baseline Requirements." This effectively means that roots that did not receive BR audits after 2013 are not eligible for inclusion. Roots with documented BR violations may also be excluded from the Mozilla root store under this policy.
- Section 8 CA Operational Changes now requires notification when an intermediate is transferred to another organization.

Please review the updates and discuss your questions and concerns with Wayne.

5 Policy Compliance and CP/CPS Updates

As part of the 2.6 policy discussions, it was decided not to define a future effective date for changes that require CAs to update their CP/CPSs. This does not mean that we are satisfied if CAs wait until they must update their CP/CPS as part of the annual review requirement. We expect CP/CPSs to reflect new BR and/or Mozilla requirements in a reasonable period of time. "Reasonable" depends on how much notice the CA has had to make the change, but in the example of the 2.6 version of policy, September (2018) is reasonable. Next year is not.

6 Enforcing commonName Deprecation

We've changed Firefox Nightly so that we no longer fall back to commonName matching in certificates within our root program. This means that the domain name or IP address in the CN must be duplicated in the SAN for the certificate to validate. This is likely to ship in either Firefox 62 or 63 [7]. We're intending to make a similar change for imported certificates later this Summer.

7 Intermediate Preloading

Later this Summer, Firefox will begin preloading its certificate database with all intermediates disclosed in the CCADB. This is an alternative to "AIA chasing" designed to reduce the incidence of "unknown issuer" errors caused by server operators neglecting to include intermediate certificates. Updates to the CCADB will be provided for Firefox users on a regular basis. We are not yet planning to use this as an enforcement mechanism for intermediate disclosures, even though the bug says that we are [8].

8 CRLite

Mozilla is planning to deploy a new revocation checking scheme called CRLite [5]. This scheme is based on CRLs and bloom filters, but uses a filter cascade to eliminate false positives. Revocation checking for both leaf and intermediate certificates will be performed via CRLite, but it does not replace OneCRL. In order for CRLite to function, Mozilla must

know about every certificate. In practice, this means that we will only enable CRLite for CAs that log all certificates issued under one or more of their roots. We believe that it is reasonable to opt-in certificates issued after April 30 by all CAs in the Mozilla program. We do expect there to be a few exceptions, but hope that they can be dealt with on a case-by-case basis. If you have concerns, please speak with Wayne or Mark. We plan to begin testing CRLite this Fall with a full rollout dependent on the results of our testing.

9 Symantec update

Firefox 60 was released on May 9th with the blocking of Symantec certificates issued prior to 1-June 2016 enabled as described in Mozilla's plan [6]. We didn't encounter any complaints. Firefox 62 (currently in the Nightly channel) includes a new option for the "security.pki.distrust_ca_policy" preference: a value of '2' enables the full distrust planned for Firefox 63 in October [7]. With this setting enabled, lots of things break, including about 7% of the top million sites.

URLs related to the above:

[1] https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/M6CafXyBBTo/DezJy2nKBgAJ
[2] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#public-audit-information
[3] https://github.com/mozilla/pkipolicy/blob/2.6/rootstore/policy.md
[4] https://github.com/mozilla/pkipolicy/compare/master...2.6
[5] https://mislove.org/publications/CRLite-Oakland.pdf
[6] https://wiki.mozilla.org/CA/Additional_Trust_Changes#Symantec
[7] https://wiki.mozilla.org/RapidRelease/Calendar
[8] https://bugzilla.mozilla.org/show_bug.cgi?id=1404934